Check Point®
SOFTWARE TECHNOLOGIES LTD

SECURE YOUR EVERYTHING™

HOW LEADERS MITIGATE CYBER SECURITY RISK
RESEARCH REVEALS SIX KEY BEST PRACTICES

Introduction

For CISOs around the globe, making decisions about their cyber security is not always clear cut. ESI ThoughtLab, a quantitative research firm, helped fill in the gaps by surveying 1000+ global CISOs.

The results are revealing. Discovered were six best practices that top firms use to stay secure in today's ever-changing security environment. Use these findings to learn how security leaders are fine tuning their security strategies to protect their industries.

ESI ThoughtLab worked with a coalition of leading cyber security technology experts to answer a central question: How can firms drive the best cyber security performance in today's complex digital world? A comprehensive benchmarking study was launched to better understand cyber security investments, practices, and performance results of 1,009 companies from 13 industries in 19 countries.

The organizations surveyed reported 28,100 successful breaches, averaging $330,000 per breach.

Cyber attack methods and costs to organizations are rising

As more businesses go digital over the next two years, executives should expect an increase in attacks through artificial intelligence (38%), denial of service (34%), and web applications (29%).
The organizations surveyed reported 28,100 successful breaches, averaging $330,000 per breach. Insurance and financial firms suffered the most attacks, with financial, retail, hospitality, and automotive firms sustaining a disproportionate number of material breaches. CISOs surveyed assigned a 45% probability of a moderate or material breach. ESI's analysis estimates that the probability is considerably higher: 62% to 86%. Below are the six key best practices to mitigate these breaches.

The Six Key Best Practices

Best practice #1: Invest more in cyber security

The more an organization can invest in the 'right' technologies and the right areas, the better the defenses. Keeping ahead of cyber threat actors means investment. Leading CISOs spend about 25 percent more than others on cyber security per employee, increasing investments annually.
They invest in different areas such as recruiting specialists, consultants, and implementing training, such as end-user security awareness training with simulated phishing.

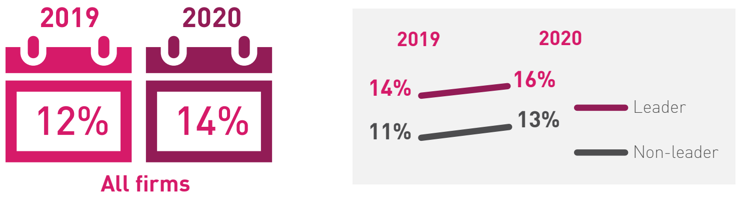
How much more are leaders spending?

While firms on average spend $9.6 million on cyber security and $515 per employee, leaders on average spend $15 million on cyber security and $618 per employee. Leaders also plan to continue their spending at a higher rates.

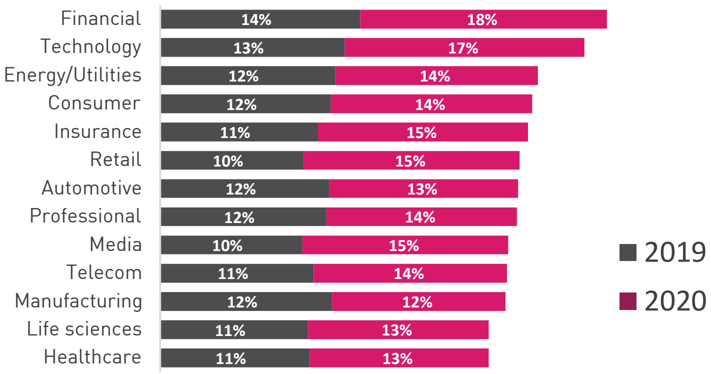
Where are leaders investing and what are they investing in?

Compared to non-leaders, leaders are more likely to make investments in training and upskilling IT staff, recruiting cyber security specialists, and compensating cyber security staff. Leaders also spend more than non-leaders on external consultants and contractors. Finally, half of leaders invest largely in external consultants and contractors.

AVERAGE INCREASE IN CYBERSECUIRTY SPENDING



AVERAGE INCREASE IN CYBERSECUIRTY BY INDUSTRY



To properly mitigate risk, leaders on average spend 25% more per employee than others and increase those investments each year.

BY COMPANY REVENUE SIZE

	Up to $1b	$1b-$4.9b	$5b-$19.9b	$20b+
Total in $M	$0.71	$2.53	$9.29	$29.16
Per Employee	$427	$444	$560	$626

BY CYBERSECURITY MATURITY

	Beginner	Implementer	Advancer	Leader	All
Total in $M	$7.50	$9.29	$11.49	$15.08	$9.58
Per Employee	$473	$430	$561	$618	$515

* All includes some respondents not classified by maturity

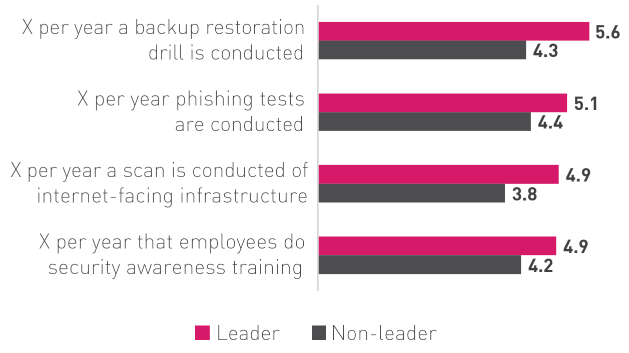
> Top leaders maintain critical patches, demonstrating the lowest percentage of unpatched "critical" or "high" vulnerabilities.

Best practice 2: Make cyber security hygiene a top priority

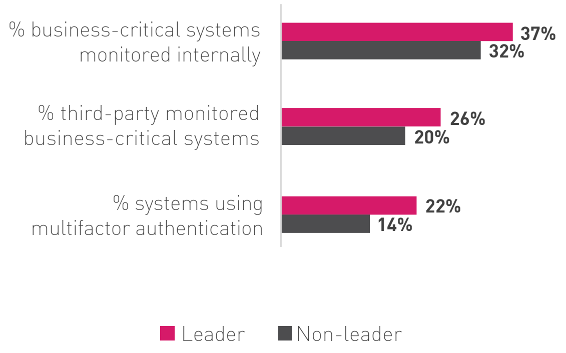
Maintaining top cyber hygiene is an essential priority that top leaders effectively implement. Top leaders maintain critical patches, demonstrating the lowest percentage of unpatched "critical" or "high" vulnerabilities. Leaders Common Vulnerability Scoring System (CVSS) scores are 18% versus 28% for others. Leaders also conduct backup restoration drills more frequently at an average of 5.6 times a year compared to 4.3 for non-leaders. They also conduct IT infrastructure scans at a rate of 4.9 versus 3.8 and phishing tests at a rate of 5.1 versus 4.4 annually.

Leaders not only take concrete steps to reduce risk through better cyber hygiene but also effectively prevent breaches through effectively completing basic tasks which improves overall performance.

NUMBER OF TIMES PER YEAR FIRMS TEST AND TRAIN



% OF SYSTEMS MAINTAINING BEST PREACTICES



In making cyber hygiene a top priority, leaders take actions such as conducting more backup restoration drills, IT infrastructure scans, and phishing tests.

CISOs at top firms focus more on four key aspects: emphasize security more than IT, role in digital transformation, managing data privacy, and prioritize operational resiliency.

Best practice 3: Keep management teams focused and aligned

Leading CISOs not only have open lines of organizational communication with leaders in their organizations, but they also manage their teams well. Heads of cyber security usually report to the CEO, COO, or the board in leader companies. CISOs at top firms also focus more on four key aspects. First, 75% of leaders emphasize security more than IT. Second, 57% of leaders play a key role in digital transformation. Third, 54% emphasize managing data privacy. Lastly, 49% prioritize operational resiliency. Leading firms are also more likely to have two executives sharing the responsibility for cyber security of the organization.

Changes in CISO role	Leader	All Others
Greater focus on security than IT	75%	68%
Bigger role in digital and business strategy	57%	45%
Expanding data privacy and compliance responsibilities	54%	42%
Greater involvement in operational resiliency	49%	41%
Increasing interaction with board/senior management	38%	32%
Partnering more with other functions, departments	36%	31%
More analytical driven in approach	30%	31%
Greater engagement in product development	30%	26%
Wider role in enterprise, geopolitical risk management	26%	25%
Bigger part in third-party/supply chain management	22%	21%
Higher stature, visibility, and managerial responsibility	18%	23%

In order to keep management teams focused and aligned, CISOs at 75% of the top firms emphasize not just IT but security as a whole.

Cybersecurity reports to:	Leader	Non-Leader
Top management		
CEO	63%	61%
COO	6%	0%
Board / board member	5%	4%
CFO	2%	0%
Other C-Suite		
CIO	17%	21%
Chief Risk Officer	4%	1%
CISO	2%	2%
CTO	1%	7%

Best practice 4: Rely heavily on advanced analytics and specialized teams

Leaders utilize advance analytics and specialized teams far more than non-leaders. What does this translate to in practice? 8 out 10 leaders take actions such as conducting cyber-risk scenario analysis, assessing the financial impact of risk events, and measuring the effects of mechanisms to mitigate cyber risks. Additionally, leaders outsource incident response, red team, risk management, and security ops more often than non-leaders.

In order to better analyze and assess, leaders invest more in cyber security technologies, focusing on data protection, firewalls, and email filtering and monitoring. Unfortunately, in the COVID-19 pandemic age, firms are underinvesting in technologies that are crucial for telework such as multi-factor authentication, disaster recovery, user behavior analytics, identity governance, and privileged access. When choosing where to invest, CISOs should identify technologies that other leaders have found to be the most effective. Leaders report the highest benefits from endpoint technology and AI-driven security orchestration. This technology facilitates updating rules and acting in real time based on machine analysis. Investment in these automated systems allows some on the decision-making to be removed from the end user, therefore protecting the enterprise where hackers most often attack.

Tech investment area	Leader	Non-Leader	Difference
Data protection	59%	59%	0%
Firewalls and web filtering	55%	48%	7%
Email filtering and monitoring	48%	37%	11%
Deception technology	42%	31%	11%
Endpoint detection and protection	39%	31%	8%
Multi-factor authentication*	38%	28%	10%
Disaster recovery*	36%	41%	-5%
Network traffic analysis	34%	32%	2%
Denial of service mitigation	33%	19%	14%
User behavior analytics*	32%	23%	9%
Intrusion detection and protection	31%	29%	2%
Identity governance*	28%	28%	0%
Cloud workload (Iaas, PaaS) security	27%	21%	6%
Cloud-access security broker (CASB)	25%	19%	6%
Privileged access management*	25%	23%	2%
Security orchestration and automation	25%	18%	7%
Encryption and tokenization	24%	18%	6%
Unified security architecture	24%	12%	12%

* Technologies crucial for remote working

8 out of 10 leader firms conduct cyber-risk scenario analysis, assess the financial impacts, and measure effects of mechanisms to mitigate cyber risks.

> Leaders gain better effectiveness from key cyber security technologies such as cloud workload security, endpoint detection, mobile device management, deception technology, email filtering, multi-factor authentication, and firewalls and web filtering.

Best practice 5: Extract greater value from cyber security tools

Leaders not only invest more, but they also invest wisely by ensuring that they get the most value form their cyber security tools. In doing this they reap the benefits and gain better effectiveness from key cyber security technologies such as cloud workload security, endpoint detection, mobile device management, deception technology, email filtering, multi-factor authentication, and firewalls and web filtering. Leaders also are adept at coordinating data security and privacy, handling backups and disaster recovery, conducting risk assessment and penetration testing, and setting out duties and governance practices.

MOST EFFECTIVE CYBERSECURITY TECHNOLOGY INVESTMENTS

	Leader	Non-Leader	Difference
Endpoint detection and protection	83%	59%	24%
Deception technology	82%	59%	23%
Data protection	75%	71%	4%
Security orchestration and automation*	71%	53%	18%
Cloud workload (Iaas, PaaS) security*	70%	46%	24%
Email filtering and monitoring software	69%	57%	12%
Firewalls and web filtering	69%	51%	18%
Mobile device management*	68%	56%	12%
Privileged access management*	68%	48%	20%
Encryption and tokenization*	66%	55%	11%

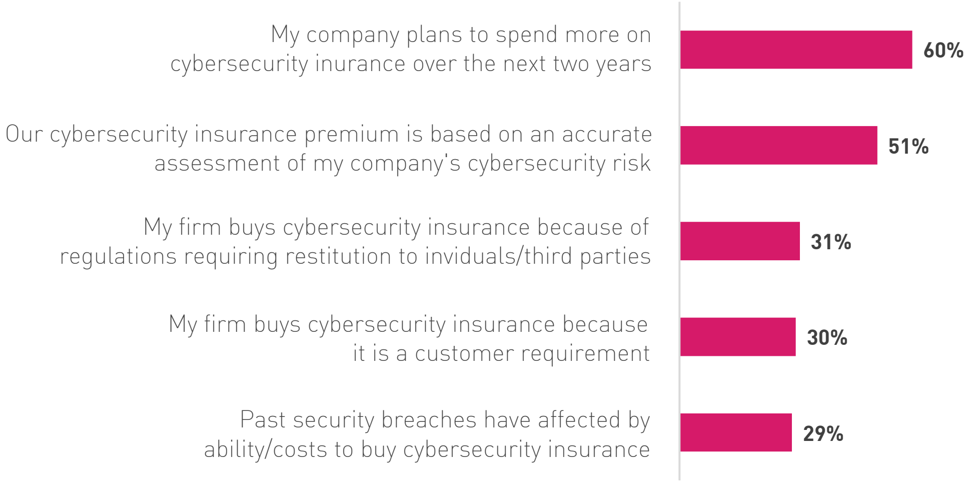
* Technology areas where only 1 in 5 firms are investing significantly

Leaders mitigate risk by investing more heavily in and achieving great effectiveness from key cyber security technologies.

Best practice 6: Make more use of cyber security insurance.

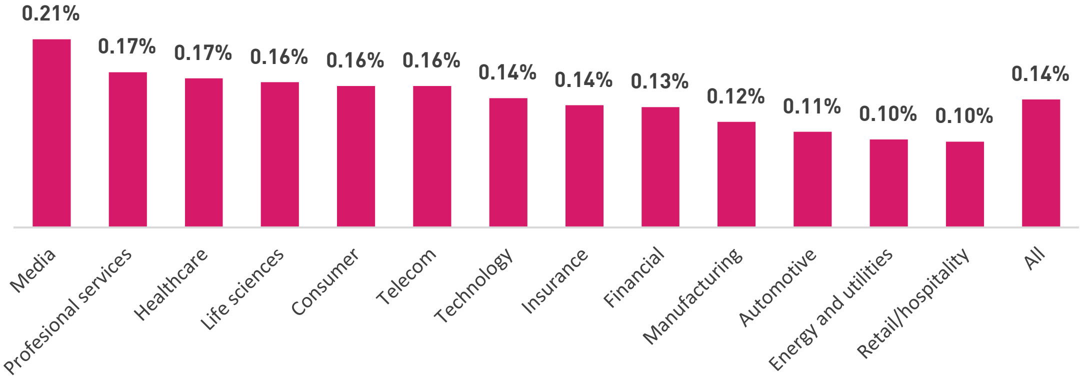
Cyber security insurance allows firms to balance how much risk they want to manage and how much they want to transfer. The average firm chooses cyber security insurance coverage that is about 0.14% of their revenue. Many firms are seeing the value in this, with 6 out of 10 firms planning to increase spending on cyber security insurance over the next two years. While insurance is not a substitute for having proper risk controls in place, it is the final key step in keeping your organization secure.

CORPORATE VIEWS ON CYBERSECURITY INSURANCE (% AGREEING)



Leaders recognize that it is impossible to mitigate all risk. Therefore, it is unsurprising that 57% of leaders have cyber insurance coverage over $10 million.

MAXIMUM CYBERSECURITY INSURANCE COVERAGE AS A % OF COMPANY REVENUE



Conclusion

These six main practices used by cyber security leaders to mitigate risks in today's fast-changing, digitally enabled environment sets apart leaders from non-leaders. The ESI report found that the firms that followed these 6 best practices, along with others, saw a high ROI. The average ROI was 179% for firms in the study. According to the surveyed firms, additional cyber security spending, which amounted to $1.4 billion, reduced their combined potential losses by an estimated $3.9 billion.

To obtain the ESI ThoughtLab Driving Cybersecurity Performance study, download from this page.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com

© 2021 Check Point Software Technologies Ltd. All rights reserved.